

The Construction of Noetherian Operators*

Ulrich Oberst

*Institut für Mathematik, Universität Innsbruck, Technikerstrasse 25,
A-6020 Innsbruck, Austria*

E-mail: Ulrich.Oberst@uibk.ac.at

Communicated by Michel Broué

Received January 22, 1999

We give an elementary and constructive, purely algebraic proof for the existence of *noetherian differential operators* for primary submodules of finite-dimensional free modules over polynomial algebras. By means of these operators the submodule can be described by differential conditions on the associated characteristic variety. This important result and the terminology are due to V. P. Palamodov. However, his, L. Ehrenpreis' and later J.-E. Björk's proofs of the existence theorem use complicated algebraic and analytic techniques and are not constructive as far as we see. The idea to characterize primary ideals by their associated differential operators is due to W. Gröbner. But M. Noether's *Fundamentalsatz* is based on similar ideas and is obviously the origin of Palamodov's terminology. © 2000 Academic Press

Key Words: Noetherian operator, differential operator, primary module, characteristic variety, Noether's Fundamentalsatz, integral representation theorem, coefficient field.

1. INTRODUCTION

We give an elementary and constructive, purely algebraic proof for the existence of *noetherian differential operators* [16] for primary submodules of finite-dimensional free modules over polynomial algebras. These operators allow one to characterize the submodule by differential conditions on the associated characteristic variety. The proofs of this important result in [16, Chap. IV, Section 3, 5, 1, Th. 8.4.5] use complicated algebraic and analytic techniques and are not constructive as far as we see. The idea to characterize primary ideals by their associated differential operators is due to W.

*Support by the Austrian FWF through Grant P13162-MAT is gratefully acknowledged.



Gröbner [6, 7]. But M. Noether's *Fundamentalsatz* [19, p. 69 of Section 92, p. 78 of Section 94] is based on similar ideas and is obviously the origin of Palamodov's terminology (see (28) below). Noetherian differential operators play an important part in the proof of the integral representation theorem which describes any solution of a linear system of partial differential equations with constant coefficients as an integral over its polynomial-exponential solutions with respect to measures whose support is contained in the characteristic variety of the system [5, 16]. The significance of this theorem and especially its constructive aspects for multidimensional systems are discussed in [14, Section 7] and [20, Section 7].

Noetherian operators are constructed in the following situation. Let $A = F[t] = F[t_1, \dots, t_n]$ be the polynomial algebra over an arbitrary field F in n indeterminates, let $J \subset A$ be a prime ideal of Krull-dimension $d := \dim(A/J)$ and let U be a J -primary submodule of the free module A^q with the factor module $M := A^q/U$. The variety of the ideal J is called the *characteristic variety* $\text{Ch}(M)$ of the module M . A polynomial belongs to J if and only if it vanishes on $\text{Ch}(M)$.

Assume first that F is of characteristic zero and consider the *n-dimensional Weyl algebra*

$$F[t, \partial_t] = F[t_1, \dots, t_n, \partial/\partial t_1, \dots, \partial/\partial t_n] \subset \text{End}_F(F[t])$$

of polynomial differential operators. If $D = (D_1, \dots, D_q) \in F[t, \partial_t]^q$ is a vectorial differential operator and if $v = (v_1, \dots, v_q)$ is a vector in $F[t]^q$ the expression $D(v) := \sum_{k=1}^q D_k(v_k) \in F[t]$ is well defined and in particular $D(v)|\text{Ch}(M) = 0$ if and only if $D(v) \in J$. The main theorem below implies that there are differential operators $D_i = (D_{i1}, \dots, D_{iq}) \in F[t, \partial_t]^q$, $i = 1, \dots, s$, such that

$$U = \{v \in F[t]^q; \text{For all } i = 1, \dots, s: D_i(v)|\text{Ch}(M) = 0\}. \quad (1)$$

In this sense U is described by differential conditions on the characteristic variety of M , for instance

$$F[t]t^m = \{v \in F[t]; \forall i = 0, \dots, m-1: (\partial^i v / \partial t^i)(0) = 0\}.$$

V. P. Palamodov [16] calls such differential operators D_i *noetherian differential operators associated with U* if they satisfy additional conditions which are needed for the proof of the integral representation theorem and which are made precise in the main theorem below. Notice that the operators D_i satisfying (1) are by no means unique.

For its further preparation let F be again an arbitrary field. According to Noether's normalization lemma there is a polynomial algebra B of dimension $d = \dim(A/J)$ such that

1. $A = B[t_H] = B[t_{d+1}, \dots, t_n]$, i.e., that A is a polynomial algebra over B .

2. $B \cap J = 0$ and A/J is a finite (= finitely generated) B -module or, in other terms, the generators $\tilde{t}_j = t_j + J \in A/J$, $j = d + 1, \dots, n$, are integral over B .

There in results the finite field extension

$$K := S^{-1}B = \text{quot}(B) \subset S^{-1}(A/J) = A_J/J_J = \text{quot}(A/J) =: k(J) \quad (2)$$

where $S := B \setminus \{0\}$. The module $M = A^q/U$ is a finite, J -coprimary A -module; hence

$$\begin{aligned} \text{Ass } M &= \{J\}, \quad J = \{a \in A; a: M \rightarrow M \text{ is nilpotent}\}, \\ S \subseteq A \setminus J &= \{s \in A; s: M \rightarrow M \text{ is injective}\}. \end{aligned} \quad (3)$$

Let $m + 1$ denote the *exponent* [19, p. 65], or index [18, p. 234], of J with respect to M , i.e., the least k such that $J^k M = 0$, and

$$I := (0: M) := (U: A^q) := \{a \in A; aM = 0\} \quad (4)$$

the annihilator of M . Since the map

$$A/I \rightarrow \text{End}_A(M), \quad \bar{a} \mapsto (x \mapsto ax),$$

is injective the ideal I is J -primary too or $\text{Ass}(A/I) = \{J\}$, i.e., every zero-divisor of A/I is nilpotent. The algebra

$$C := S^{-1}(A/I) = S^{-1}A/S^{-1}I = (A/I)_J = A_J/I_J \supset \mathfrak{m} := S^{-1}J/S^{-1}I \quad (5)$$

is a finite-dimensional, local K -algebra with maximal ideal $\mathfrak{m} = S^{-1}J/S^{-1}I$ of exponent $m + 1$ and residue field

$$C/\mathfrak{m} = S^{-1}A/S^{-1}J = A_J/J_J = k(J). \quad (6)$$

Let

$$L := C_{\text{sep}} := \{c \in C; c \text{ is separable over } K\} \subset C \quad (7)$$

denote the separable closure of K in C . Since C is local L is a separable field extension of K , and the canonical map $C \rightarrow C/\mathfrak{m}$ induces the isomorphism

$$\text{can}: L \cong k(J)_{\text{sep}}, \quad c \mapsto \bar{c} := c + \mathfrak{m},$$

where $k(J)_{\text{sep}}$ is the separable closure of K in $k(J)$. The module $S^{-1}M = M_J$ is a C -, $S^{-1}A$ -, and A_J -module of finite length or *multiplicity*

$$s := \text{length}_{A_J}(M_J) = [S^{-1}M: L]/[k(J): L] = [S^{-1}M: K]/[k(J): K] \quad (8)$$

and contains M since $S = B \setminus \{0\}$ consists of non-zero-divisors of M . In particular, there is an L -isomorphism

$$\phi: S^{-1}M \cong k(J)^s = S^{-1}(A/J)^s. \quad (9)$$

MAIN THEOREM AND DEFINITION 1 (construction of noetherian operators). *Data as introduced above.*

(i) Any L -linear isomorphism $\phi: S^{-1}M \cong k(J)^s = S^{-1}(A/J)^s$ is a K -linear differential operator. There is an $s_0 \in S$ such that $s_0 \phi(M) \subset (A/J)^s$, and then

$$\bar{D} := s_0 \phi \text{ can}: A^q \rightarrow M = A^q/U \xrightarrow{s_0 \phi} (A/J)^s$$

is a B -linear differential operator. Since A is a polynomial algebra over B the differential operator \bar{D} can be lifted to a B -linear differential operator

$$D = (D_{ik})_{i,k}: A^q \rightarrow A^s, \quad v = (v_1, \dots, v_q)^T \mapsto \left(\sum_{k=1}^q D_{ik}(v_k) \right)_{i=1, \dots, s},$$

with components $D_{ik}: A \rightarrow A$ such that the diagram

$$\begin{array}{ccccc} A^q & \xrightarrow{\text{can}} & M = A^q/U & \xrightarrow{\text{inj}} & S^{-1}M \\ \downarrow D & & \downarrow s_0 \phi & & \downarrow s_0 \phi \\ A^s & \xrightarrow{\text{can}} & (A/J)^s & \xrightarrow{\text{inj}} & k(J)^s \end{array}$$

commutes. In other terms, the B -linear differential operator D induces the B -monomorphism

$$D_{\text{ind},1} = s_0 \phi: M = A^q/U \rightarrow (A/J)^s, \quad s := \text{length}_{A_J}(M_J), \quad \text{or}$$

$$U = \left\{ v = (v_1, \dots, v_q)^T \in A^q; \text{ for all } i = 1, \dots, s: \sum_{k=1}^q D_{ik}(v_k) \in J \right\},$$

and the L -isomorphism

$$D_{\text{ind},2} = s_0 \phi: S^{-1}M \rightarrow S^{-1}(A/J)^s.$$

According to V. P. Palamodov [16, ch. IV, §4, def. 1, cor. 2], the differential operator D is called a **noetherian operator** for the coprimary module M resp. the primary submodule U of A^q . The condition $\sum_{k=1}^q D_{ik}(v_k) \in J$ can be and is usually expressed as

$$\sum_{k=1}^q D_{ik}(v_k) | \text{Ch}(M) = 0,$$

$$\text{Ch}(M) := \text{Var}(I) = \text{Var}(J) := \{ \zeta \in \bar{F}^n; \forall P \in I: P(\zeta) = 0 \}$$

where \bar{F} denotes the algebraic closure of F and $\text{Ch}(M) = \text{Var}(I)$ the characteristic variety of M .

(ii) If the extension $K = S^{-1}B \subset k(J)$ is separable as, for instance, always in characteristic zero the differential operator \bar{D} is and the operator D can be chosen of order m where $m + 1$ is the exponent of J with respect to M satisfying $J^{m+1}M = 0$.

(iii) If $D, \tilde{D}: A^q \rightarrow A^s$ are two B -linear noetherian differential operators for $M = A^q/U$, i.e., if

$$U = \{v \in A^q; D(v) \in J^{\times s}\} = \{v \in A^q; \tilde{D}(v) \in J^{\times s}\},$$

$$s = \text{length}_{A_J}(M_J),$$

then there is a unique L -automorphism $\Psi \in \text{Gl}_L(k(J)^s)$ such that

$$\Psi \circ \text{can} \circ D = \text{can} \circ \tilde{D}, \quad \text{can}: A^s \rightarrow (A/J)^s \subset k(J)^s.$$

The B -linearity of the operators D_{ij} of the preceding theorem is decisive in context with the integral representation theorem, and therefore Palamodov uses the noetherian operator terminology only for operators with the properties of the preceding theorem and not for all operators satisfying (1).

The existence part, but not the construction of the preceding theorem is due to V. P. Palamodov for the ground field \mathbb{C} . W. Gröbner formulated the problem of the theorem for general primary ideals in characteristic zero in [7, p. 130], and proved it for prime ideals in [6] and for zero-(Krull-)dimensional primary ideals whose roots are rational maximal ideals in [8, pp. 174–178], by a simple application of Macaulay's inverse systems. The special case of zero-(Krull-)dimensional ideals has been taken up by M. G. Marinari *et al.* [11] under the name "Gröbner duality," the noetherian operators being called differential conditions. R. Brommer [3] also gave a purely algebraic existence proof for the representation (1) in case A is an algebra essentially of finite type over a perfect field, J is a regular prime ideal of A , and U is a J -primary ideal of A , but without referring to [1, 5, 16]; H. Reitberger pointed out this reference. R. Brommer also used the differential calculus exposed in Section 2. Recently P. Hackmann [9] gave a further purely algebraic existence proof for an algebraically closed base field of characteristic zero by means of a precise description of the indecomposable injective envelope $E(A/J)$. For zero-(Krull-)dimensional or maximal prime ideals J these modules were also described in [15] as modules of polynomial-exponential functions.

The new constructive proof of the theorem relies on three simple, but decisive observations:

1. As explained above the general J -coprimary module M can be reduced to the zero-(Krull-) or K -finite-dimensional module $S^{-1}M$ with the associated maximal ideal $S^{-1}J$. This reduction procedure was already used in [19, Section 94], and was also used in Palamodov's and Björk's proof of the existence of noetherian operators [16, Ch. IV, Section 3, p. 161, 1, Ch. 8, Section 4, p. 350].

2. Any L -linear map as in (9) is a K -linear differential operator.

3. The B -module $\text{Diff}_{A/B}(M, N)$ of B -linear differential operators between A -modules M and N is a functor of these modules.

Theorem 1 is proven in Section 4. Algorithm 15 sums up all necessary construction steps. In Eqs. (27) and (28) we explain the connection of the theorem with M. Noether's *Fundamentalsatz*. The needed effective computations are taken from W. Vasconcelos' book [18] and are discussed in Remark 17. In Section 2 we explain the needed elementary theory of differential operators as exposed in the book [4] by M. Demazure and P. Gabriel, and in Section 3 we apply this to finite-dimensional local algebras and in particular to $C = S^{-1}(A/I)$.

2. DIFFERENTIAL OPERATORS

This section is an adaption of [4, Ch. II, Section 4.5]. Let B be any commutative ring and A a commutative B -algebra. An $A \otimes_B A$ -module X is an A - A -bimodule X with

$$(a_1 \otimes a_2) \circ x = a_1 x a_2, \quad bx = xb \text{ for } b \in B.$$

In particular, A itself is an $A \otimes_B A$ -bimodule and, conversely, $A \otimes_B A$ is a left and a right A -module via

$$\begin{aligned} \text{inj}_1: A &\rightarrow A \otimes_B A, & a &\mapsto a \otimes 1, & a(a_1 \otimes a_2) &:= aa_1 \otimes a_2, \\ \text{inj}_2: A &\rightarrow A \otimes_B A, & a &\mapsto 1 \otimes a, & (a_1 \otimes a_2)a &:= a_1 \otimes a_2 a. \end{aligned}$$

LEMMA AND DEFINITION 2. *The multiplication map*

$$A \otimes_B A \rightarrow A, \quad a_1 \otimes a_2 \mapsto a_1 a_2$$

is $A \otimes_B A$ -linear and an algebra epimorphism, and hence its kernel $I_{A/B}$ is an ideal of $A \otimes_B A$ and indeed

$$I_{A/B} = \sum_{a \in A} A(1 \otimes a - a \otimes 1) \quad \text{and}$$

$$I_{A/B}^{m+1} = \sum_{a_0, \dots, a_m \in A} A(1 \otimes a_0 - a_0 \otimes 1) * \dots * (1 \otimes a_m - a_m \otimes 1)$$

for all $m \geq 0$.

Proof. If $\sum_i a_i \otimes b_i \in I_{A/B}$ then $\sum_i a_i b_i = 0 \in A$ and

$$\sum_i a_i \otimes b_i = \sum_i a_i \otimes b_i - \sum_i a_i b_i \otimes 1 = \sum_i a_i (1 \otimes b_i - b_i \otimes 1).$$

■

For any $A \otimes_B A$ -module X we define the B -linear derivation

$$\text{ad}: A \rightarrow \text{End}_B(X), a \mapsto \text{ad}(a), \quad \text{ad}(a)(x) := xa - ax,$$

which satisfies the product rule

$$\text{ad}(a_1 a_2) = \text{ad}(a_1)(1 \otimes a_2) + (a_1 \otimes 1)\text{ad}(a_2) \quad \text{or}$$

$$\text{ad}(a_1 a_2)(x) = \text{ad}(a_1)(x)a_2 + a_1 \text{ad}(a_2)(x).$$

The annihilator

$$\begin{aligned} (0: I_{A/B}^{m+1})_X &:= \{x \in X; \text{For all } c \in I_{A/B}^{m+1}: c \circ x = 0\} \\ &= \{x \in X; \forall a_0, \dots, a_m \in A: (1 \otimes a_0 - a_0 \otimes 1) \\ &\quad * \dots * (1 \otimes a_m - a_m \otimes 1) \circ x = 0\} \\ &= \{x \in X; \forall a_0, \dots, a_m \in A: \text{ad}(a_0) \circ \dots \circ \text{ad}(a_m)(x) = 0\} \end{aligned} \quad (10)$$

is an $A \otimes_B A$ -submodule of X . Consider, in particular, for A -modules M and N , the $A \otimes_B A$ -bimodule $\text{Hom}_B(M, N)$ with the structure

$$[(a_1 \otimes a_2) \circ D](x) := a_1 D(a_2 x), \quad \text{ad}(a)(D)(x) = D(ax) - aD(x),$$

for $a_1, a_2, a \in A$, $D \in \text{Hom}_B(M, N)$ and $x \in M$.

DEFINITION 3. The $A \otimes_B A$ -submodule

$$\begin{aligned} \text{Diff}_{A/B}^m(M, N) &:= (0: I_{A/B}^{m+1})_{\text{Hom}_B(M, N)} \\ &= \{D \in \text{Hom}_B(M, N); \forall a_0, \dots, a_m \\ &\quad \in A: \text{ad}(a_0) \circ \dots \circ \text{ad}(a_m)(D) = 0\} \end{aligned}$$

of $\text{Hom}_B(M, N)$ is called the module of B -linear differential operators of order (at most) m from M to N , in particular

$$\text{Diff}_{A/B}^0(M, N) = \text{Hom}_A(M, N).$$

Likewise the module

$$\text{Diff}_{A/B}(M, N) := \text{Diff}_{A/B}^\infty(M, N) := \bigcup_{m=0}^{\infty} \text{Diff}_{A/B}^m(M, N)$$

is the $A \otimes_B A$ -module of all B -linear differential operators from M to N .

If $f: M_1 \rightarrow M$ and $g: N \rightarrow N_1$ are A -linear the B -linear map

$$\text{Hom}(f, g): \text{Hom}_B(M, N) \rightarrow \text{Hom}_B(M_1, N_1), \quad D \mapsto g \circ D \circ f,$$

is indeed $A \otimes_B A$ -linear and induces the $A \otimes_B A$ -linear map

$$\text{Diff}_{A/B}^m(f, g): \text{Diff}_{A/B}^m(M, N) \rightarrow \text{Diff}_{A/B}^m(M_1, N_1), \quad 0 \leq m \leq \infty. \quad (11)$$

In other words, $\text{Diff}_{A/B}^m(-, -)$ is a left exact functor. For $0 \leq m < \infty$ it is representable. Indeed, the canonical isomorphism

$$\begin{aligned} \text{Hom}_A(A \otimes_B M, N) &\cong \text{Hom}_B(M, N), & \Phi &\leftrightarrow D, \\ \Phi(a \otimes x) &= aD(x), & a &\in A, \quad x \in M, \end{aligned} \quad (12)$$

is $A \otimes_B A$ -linear too, the $A \otimes_B A$ -structure on the left being derived from that of $A \otimes_B M$ given by $(a_1 \otimes a_2)(a \otimes x) := a_1 a \otimes a_2 x$. The map

$$d^m: M \rightarrow P_{A/B}^m(M) := (A \otimes_B M) / I_{A/B}^{m+1} \circ (A \otimes_B M), \quad x \mapsto \overline{1 \otimes x},$$

is the universal B -linear differential operator of order (at most) m ; i.e., (12) induces the functorial isomorphism

$$\begin{aligned} \text{Hom}_A(P_{A/B}^m(M), N) &\cong \text{Diff}_{A/B}^m(M, N), & \phi &\leftrightarrow D, \\ D &= \phi \circ d^m, & \phi(\overline{a \otimes x}) &= aD(x), & a &\in A, \quad x \in M. \end{aligned}$$

For $M = A$ there in results the universal m th order differential operator

$$d^m: A \rightarrow P^m(A/B) := P_{A/B}^m(A) = (A \otimes_B A) / I_{A/B}^{m+1}, \quad a \mapsto \overline{1 \otimes a},$$

and the isomorphism

$$\begin{aligned} \text{Hom}_A(P^m(A/B), N) &\cong \text{Diff}_{A/B}^m(A, N), & \phi &\leftrightarrow D, \\ D(a) &= \phi(\overline{1 \otimes a}). \end{aligned}$$

EXAMPLE 4. If $A = B[t] = B[t_1, \dots, t_r]$ is a polynomial algebra the module $P^m(A/B)$ is A -free. Indeed

$$\begin{aligned} A \otimes_B A &= B[t] \otimes_B B[t] = B[t_i \otimes 1, 1 \otimes t_i]_{i=1, \dots, r} \\ &= B[t_i \otimes 1, 1 \otimes t_i - t_i \otimes 1]_{i=1, \dots, r} = B[t_1, \dots, t_r, h_1, \dots, h_r] \\ &= B[t, h] \end{aligned}$$

where $t_i \otimes 1 = (\text{identification})t_i$ and $h_i := 1 \otimes t_i - t_i \otimes 1$

is also a polynomial algebra in $2r$ indeterminates t_i and h_i . With this identification the ideal $I_{A/B}$ is given as

$$I_{B[t]/B} = \sum_{i=1}^r B[t, h]h_i, \quad I_{B[t]/B}^{m+1} = \sum_{\alpha} \{B[t, h]h^{\alpha}; \alpha \in \mathbb{N}^r, |\alpha| = m+1\}$$

where $\alpha = (\alpha_1, \dots, \alpha_r) \in \mathbb{N}^r$, $h^{\alpha} := h_1^{\alpha_1} * \dots * h_r^{\alpha_r}$ and $|\alpha| := \alpha_1 + \dots + \alpha_r$. The second injection from A into $A \otimes_B A$ is

$$\text{inj}_2: B[t] \rightarrow A \otimes_B A = B[t, h] = \bigoplus_{\alpha \in \mathbb{N}^r} B[t]h^{\alpha},$$

$$P = P(t) \mapsto 1 \otimes P(t) = P(1 \otimes t) = P(t + h) = \sum_{\alpha \in \mathbb{N}^r} (D^{\alpha}P)(t)h^{\alpha}$$

with

$$D^{\alpha}t^{\beta} = \begin{cases} \binom{\beta}{\alpha} t^{\beta-\alpha} & \text{if } \alpha \leq \beta, \\ 0 & \text{otherwise,} \end{cases} \quad (13)$$

in particular

$$D^{\alpha} = \frac{1}{\alpha!} \partial^{|\alpha|} / \partial t^{\alpha} \quad \text{if } \mathbb{Q} \subset B \subset A,$$

where $\alpha \leq \beta$ signifies that $\alpha_i \leq \beta_i$ for all $i = 1, \dots, r$. There in results the universal B -linear differential operator of order m

$$d^m: B[t] \rightarrow P^m(B[t]/B) = \bigoplus_{|\alpha| \leq m} B[t] \overline{h^{\alpha}}$$

$$P \mapsto \overline{P(t+h)} = \sum_{|\alpha| \leq m} (D^{\alpha}P)(t) \overline{h^{\alpha}}$$

where $P^m(B[t]/B)$ is a free $B[t]$ -module with the basis $\overline{h^{\alpha}}$, $\alpha \in \mathbb{N}^r$, $|\alpha| \leq m$. The equations

$$h^{\alpha} = (t + h - t)^{\alpha} = \sum_{\beta \leq \alpha} \binom{\alpha}{\beta} (t + h)^{\beta} (-t)^{\alpha-\beta}, \quad \text{hence}$$

$$\overline{h^{\alpha}} = \sum_{\beta \leq \alpha} \binom{\alpha}{\beta} (-t)^{\alpha-\beta} \overline{(t+h)^{\beta}} = \sum_{\beta \leq \alpha} \binom{\alpha}{\beta} (-t)^{\alpha-\beta} d^m(t^{\beta}) \quad (14)$$

imply that the vectors $d^m(t^\alpha)$, $|\alpha| \leq m$, are also an A -basis of $P^m(A/B)$, i.e.,

$$P^m(B[t]/B) = \bigoplus_{\alpha \in \mathbb{N}^r, |\alpha| \leq m} B[t] \bar{h}^\alpha = \bigoplus_{\alpha \in \mathbb{N}^r, |\alpha| \leq m} B[t] d^m(t^\alpha),$$

$$d^m(P) = \sum_{|\alpha| \leq m} (D^\alpha P) \bar{h}^\alpha = \sum_{\beta \leq \alpha, |\alpha| \leq m} (D^\alpha P) \binom{\alpha}{\beta} (-t)^{\alpha-\beta} d^m(t^\beta). \quad (15)$$

In other words, for every choice of vectors $y_\alpha \in N$, $\alpha \in \mathbb{N}^r$, $|\alpha| \leq m$, there is a unique B -linear differential operator $D: B[t] \rightarrow N$ of order at most m such that

$$D(t^\alpha) = y_\alpha \quad \text{for all } \alpha \in \mathbb{N}^r, |\alpha| \leq m, \quad \text{viz.,}$$

$$D(P) = \sum_{\beta \leq \alpha, |\alpha| \leq m} (D^\alpha P) \binom{\alpha}{\beta} (-t)^{\alpha-\beta} y_\beta. \quad (16)$$

Moreover, given any A -epimorphism $g: N_1 \rightarrow N_2$, every B -linear differential operator $D_2: B[t] \rightarrow N_2$ of order m can be lifted to a B -linear differential operator $D_1: B[t] \rightarrow N_1$ of the same order with $g \circ D_1 = D_2$.

We need the following behavior of differential operators under localization. Assume that B is noetherian, S is a multiplicative submonoid of B , and M and N are A -modules which are finite as B -modules. We use the standard identification

$$S^{-1} \operatorname{Hom}_B(M, N) = \operatorname{Hom}_B(S^{-1}M, S^{-1}N) = \operatorname{Hom}_{S^{-1}B}(S^{-1}M, S^{-1}N),$$

$$\frac{D}{s} = s^{-1}(S^{-1}D), \quad (S^{-1}D)\left(\frac{x}{t}\right) = \frac{D(x)}{t}$$

which induces the inclusion

$$\begin{aligned} S^{-1} \operatorname{Diff}_{A,B}^m(M, N) &\subset \operatorname{Diff}_{A/B}^m(S^{-1}M, S^{-1}N) \\ &= \operatorname{Diff}_{S^{-1}A/S^{-1}B}^m(S^{-1}M, S^{-1}N). \end{aligned}$$

If N is S -torsionfree, i.e., if $sy = 0$ implies $y = 0$ for $s \in S$ and $y \in N$, then so is $\operatorname{Hom}_B(M, N)$ and then

$$\begin{aligned} S^{-1} \operatorname{Diff}_{A,B}^m(M, N) &= \operatorname{Diff}_{A/B}^m(S^{-1}M, S^{-1}N) \\ &= \operatorname{Diff}_{S^{-1}A/S^{-1}B}^m(S^{-1}M, S^{-1}N). \end{aligned} \quad (17)$$

The following result can, for instance, be derived from [12, Sections 25–26], but we give a simple direct proof. The multiplication map $a_1 \otimes a_2$

$\mapsto a_1 a_2$ admits the left A -linear section $a \mapsto a \otimes 1$, and thus induces the direct decomposition

$$A \otimes_B A = A(\overline{1 \otimes 1}) \oplus I_{A/B}, \quad a_1 \otimes a_2 = a_1 a_2 \otimes 1 + a_1(\overline{1 \otimes a_2 - a_2 \otimes 1}),$$

$$P^1(A/B) = A(\overline{1 \otimes 1}) \oplus \Omega(A/B), \quad \Omega(A/B) := I_{A/B}/I_{A/B}^2,$$

$$d^1(a) = \overline{1 \otimes a} = a(\overline{1 \otimes 1}) + d(a), \quad d(a) := \overline{1 \otimes a - a \otimes 1},$$

of A -modules. For an arbitrary A -module N the A -module

$$\text{Der}_B(A, N) := \{D \in \text{Hom}_B(A, N); D(a_1 a_2) = a_2 D(a_1) + a_1 D(a_2)\}$$

of B -linear derivations from A to N coincides with $\{D \in \text{Diff}_{A/B}^1(A, N); D(1) = 0\}$. This implies that the universal differential operator d^1 of order one induces the universal B -linear derivation

$$d: A \rightarrow \Omega(A/B), \quad a \mapsto d(a) = d^1(a) - a(\overline{1 \otimes 1}),$$

i.e., the functorial isomorphism

$$\text{Hom}_A(\Omega(A/B), N) \cong \text{Der}_B(A, N), \quad \Psi \leftrightarrow D, \quad D(a) = \Psi(d(a)),$$

holds. From Lemma 2 we get

$$\Omega(A/B) = \text{Ad}(A) = \sum_{a \in A} \text{Ad}(a).$$

LEMMA 5. If $A = B[a_1, \dots, a_r]$ then $\Omega(A/B) = \sum_{i=1}^r \text{Ad}(a_i)$.

Proof. Let $a = f(a_1, \dots, a_r) \in A$ be any element where $f \in B[t_1, \dots, t_r]$ is a polynomial. The derivation d satisfies the product rule; hence

$$d(a) = \sum_{i=1}^r \partial f / \partial t_i(a_1, \dots, a_r) d(a_i) \quad \text{and}$$

$$\Omega(A/B) = \sum_{a \in A} \text{Ad}(a) = \sum_{i=1}^r \text{Ad}(a_i).$$

■

THEOREM 6. If $K \subset L$ is a finite-dimensional separable field extension then

$$\text{Hom}_L(M, N) = \text{Diff}_{L/K}^0(M, N) = \text{Diff}_{L/K}(M, N)$$

for all L -spaces M and N .

Proof. Recall that

$$\text{Diff}_{L/K}^m(M, N) = (0 : I_{L/K}^{m+1})_{\text{Hom}_K(M, N)}$$

for all M and N and in particular

$$\text{Diff}_{L/K}^0(M, N) = (0 : I_{L/K})_{\text{Hom}_K(M, N)} = \text{Hom}_L(M, N).$$

Therefore it suffices to show that $I_{L/K} = I_{L/K}^2$ or $\Omega(L/K) = 0$. But L admits a primitive element α ; hence $L = K[\alpha]$ and $\Omega(L/K) = Ld(\alpha)$. Since the extension $K \subset L$ is assumed separable the minimal polynomial $f \in K[t]$ of α has α as a simple root and thus $f'(\alpha) \neq 0$. The equation $f(\alpha) = 0$ finally implies

$$0 = d(f(\alpha)) = f'(\alpha)d(\alpha), \quad \text{hence } d(\alpha) = 0 \quad \text{and} \quad \Omega(L/K) = 0.$$

■

3. DIFFERENTIAL OPERATORS AND DUALITY FOR FINITE-DIMENSIONAL LOCAL ALGEBRAS

In this section we assume that C is a finite-dimensional local K -algebra over a field K with maximal ideal \mathfrak{m} of exponent $m+1$, $\mathfrak{m}^{m+1} = 0$, and residue field C/\mathfrak{m} . Under the hypotheses of Theorem 1 this situation is obtained by applying the localization functor $S^{-1}(-)$, $S := B \setminus \{0\}$, to the F -algebra A/I , $I = (0 : M)$. Let

$$L := C_{\text{sep}} := \{c \in C; c \text{ is separable over } K\}$$

denote the separable closure of K in C . Here an element $c \in C$ is called separable over K if its minimal polynomial has only simple roots in an algebraic closure of K or, equivalently, if $K[c]$ is a finite product of separable field extensions of K . Since C is local C_{sep} is itself a separable field extension of K , and the canonical map $\text{can}: C \rightarrow C/\mathfrak{m}$ induces a K -monomorphism

$$\text{can}: L = C_{\text{sep}} \rightarrow (C/\mathfrak{m})_{\text{sep}}, \quad c \mapsto \bar{c} := c + \mathfrak{m}. \quad (18)$$

LEMMA 7. *The canonical map (18) is an isomorphism. More precisely, if $\gamma \in (C/\mathfrak{m})_{\text{sep}}$ has the minimal polynomial $f \in K[X]$ (with $f'(\gamma) \neq 0$) then there is a unique root c of f in C above γ , i.e., satisfying $\bar{c} = \gamma$ and $f(c) = 0$. The map*

$$\sigma: (C/\mathfrak{m})_{\text{sep}} \rightarrow C_{\text{sep}}, \quad \gamma \mapsto \sigma(\gamma) := c$$

is the section of the canonical map $C_{\text{sep}} \rightarrow (C/\mathfrak{m})_{\text{sep}}$.

Proof. The result and proof are standard. We repeat the proof given in [17, Chap. II, Section 4, Prop. 7] since the construction of σ is needed for the construction of the noetherian operators in the main theorem 1.

If $\bar{c} = \gamma$ the inequality $\overline{f'(c)} = f'(\gamma) \neq 0$ implies

$$f'(c) \in C \setminus \mathfrak{m} = U(C) := \text{group of units of } C.$$

If c and $c + h$, $h \in \mathfrak{m}$, are roots of f above γ then

$$0 = f(c + h) - f(c) = f'(c)h + h^2\hat{c}, \quad \hat{c} \in C,$$

or

$$h = -f'(c)^{-1}h^2\hat{c} \in C * h^2.$$

Since $h \in \mathfrak{m}$ and \mathfrak{m} is nilpotent this implies $h = 0$ and the uniqueness of the root c of f above γ .

To show the existence of such a root choose any c_0 with $\bar{c}_0 = \gamma$ and define the sequence c_0, c_1, \dots by Newton's procedure

$$c_{k+1} := c_k - f'(c_k)^{-1}f(c_k), \quad k = 0, 1, \dots$$

Inductively one obtains

$$f(c_k) \equiv 0(\mathfrak{m}^{2^k}) \quad \text{and} \quad c_{k+1} \approx c_k(\mathfrak{m}^{2^k}),$$

in particular $\bar{c}_k = \gamma$ for all $k \geq 0$. But $\mathfrak{m}^{m+1} = 0$; hence $f(c_p) = 0$ and $\bar{c}_p = \gamma$ if $2^p \geq m + 1$. The isomorphism

$$K[X]/K[X]f \cong K[c] \cong K[\gamma], \quad \bar{X} \mapsto c := c_p \mapsto \gamma,$$

implies that c is separable; hence $c \in L = C_{\text{sep}}$ and $\bar{c} = \gamma$. ■

COROLLARY 8. If $\gamma_1, \dots, \gamma_t$ are a K -basis of $(C/\mathfrak{m})_{\text{sep}}$ then $c_1 := \sigma(\gamma_1), \dots, c_t := \sigma(\gamma_t)$ are a K -basis of $L = C_{\text{sep}}$.

COROLLARY 9. If the residue field C/\mathfrak{m} of C is separable over K as, for instance, always in characteristic zero then L is a coefficient field of C , i.e.,

$$L \cong C/\mathfrak{m}, \quad c \mapsto \bar{c}, \quad \text{or} \quad C = L \oplus \mathfrak{m},$$

and indeed the unique one containing K .

If the extension $K \subset C/\mathfrak{m}$ is not separable C still has a coefficient field as an equicharacteristic complete local ring [12, Th. 28.3], but this does not contain K in general as we need it here. The following theorem holds without any separability assumptions.

THEOREM 10. If C is a finite-dimensional local K -algebra and $L := C_{\text{sep}}$ is the separable closure of K in C/\mathfrak{m} then

$$\text{Hom}_L(M, N) = \text{Diff}_{C/K}(M, N)$$

for all C -modules M and N . If, in addition, the maximal ideal \mathfrak{m} of C has the exponent $m + 1$, $\mathfrak{m}^{m+1} = 0$, and if the residue field extension $K \subset C/\mathfrak{m}$ is separable then

$$\mathrm{Hom}_L(M, C/\mathfrak{m}) = \mathrm{Diff}_{C/K}^m(M, C/\mathfrak{m}) = \mathrm{Diff}_{C/L}^m(M, C/\mathfrak{m})$$

for all C -modules M .

Proof. (i) Since $K \subset L$ is separable Theorem 6 yields the first inclusion

$$\mathrm{Diff}_{C/K}(M, N) \subset \mathrm{Diff}_{L/K}(M, N) = \mathrm{Diff}_{L/K}^0(M, N) = \mathrm{Hom}_L(M, N).$$

(ii) We prove that the ideal $I_{C/L}$ or all its generators $1 \otimes c - c \otimes 1 \in C \otimes_L C$ are nilpotent from which we then infer

$$\mathrm{Hom}_L(M, N) = \mathrm{Diff}_{C/L}(M, N) \subset \mathrm{Diff}_{C/K}(M, N)$$

as asserted.

Assume first that C is a field. If this is separable over K or $L = C$ the equality $I_{L/L} = 0$ is obvious. This holds if the characteristic p of K is zero. If $p > 0$ the extension $L \subset C$ is purely inseparable and there is an index e such that $c^{p^e} \in L$ for all $c \in C$. This implies that

$$(1 \otimes c - c \otimes 1)^{p^e} = 1 \otimes c^{p^e} - c^{p^e} \otimes 1 = 0 \in C \otimes_L C$$

from which the nilpotency of $I_{C/L}$ follows.

In general the maximal ideal \mathfrak{m} of C is nilpotent and so is the kernel

$$\mathfrak{m} \otimes C + C \otimes \mathfrak{m} = \ker(C \otimes_L C \rightarrow \bar{C} \otimes_L \bar{C}, c_1 \otimes c_2 \mapsto \bar{c}_1 \otimes \bar{c}_2)$$

where $\bar{C} := C/\mathfrak{m}$ denotes the residue field. But according to the preceding argument any element $1 \otimes \bar{c} - \bar{c} \otimes 1$, $c \in C$, is nilpotent in $\bar{C} \otimes_L \bar{C}$. Hence there is an index k such that

$$(1 \otimes c - c \otimes 1)^k \in \mathfrak{m} \otimes C + C \otimes \mathfrak{m}.$$

The nilpotency of the latter kernel ideal implies that $1 \otimes c - c \otimes 1$ is nilpotent as asserted.

(iii) Assume finally that $K \subset C/\mathfrak{m}$ is separable so that L is a coefficient field of C or $C = L \oplus \mathfrak{m}$. For $c = l + x \in C = L \oplus \mathfrak{m}$ this implies $\mathrm{ad}(c) = \mathrm{ad}(x)$ since $1 \otimes l - l \otimes 1 = 0 \in C \otimes_L C$. For every L -linear map $\phi: M \rightarrow C/\mathfrak{m}$ this yields

$$\mathrm{ad}(c)(\phi)(y) = \mathrm{ad}(x)(\phi)(y) = \phi(xy) - x\phi(y) = \phi(xy), \quad y \in M,$$

since $x\phi(y) \in \mathfrak{m}(C/\mathfrak{m}) = 0$. For $m + 1$ elements

$$c_i = l_i + x_i \in C = L \oplus \mathfrak{m}, \quad i = 0, \dots, m,$$

this gives

$$\mathrm{ad}(c_0) \circ \cdots \circ \mathrm{ad}(c_m)(\phi)(y) = \phi(x_0 * \cdots * x_m * y) = 0$$

since $x_0 * \cdots * x_m \in \mathfrak{m}^{m+1} = 0$. Hence

$$\begin{aligned} \mathrm{Hom}_L(M, C/\mathfrak{m}) &\subseteq \mathrm{Diff}_{C/L}^m(M, C/\mathfrak{m}) \subseteq \mathrm{Diff}_{C/K}(M, C/\mathfrak{m}) \\ &= \mathrm{Hom}_L(M, C/\mathfrak{m}). \end{aligned}$$

■

COROLLARY 11. *In the situation of Theorem 10 let N be a finite C -module of length s . Then*

$$s = \mathrm{length}_C(N) = [N : L] / [(C/\mathfrak{m}) : L] = [N : K] / [(C/\mathfrak{m}) : K], \quad (19)$$

and any L -linear isomorphism $\Phi: N \cong (C/\mathfrak{m})^s$ is indeed a K -linear differential operator. If the additional conditions of the theorem are satisfied it is of order at most m .

Proof. Only Eq. (19) has to be shown. But this follows directly from a composition series

$$N = N_0 \supset N_1 \supset \cdots \supset N_s = 0 \quad \text{with factors } N_{i-1}/N_i \cong C/\mathfrak{m}.$$

■

For the following construction of a special L -isomorphism $\Phi: N \cong (C/\mathfrak{m})^s$ we assume that the residue field extension $K \subset (C/\mathfrak{m})$ is separable and hence

$$C = L \oplus \mathfrak{m}, \quad s = \mathrm{length}_C(N) = [N : L].$$

Let $\gamma_1, \dots, \gamma_t$, $t := [(C/\mathfrak{m}) : K]$, be a K -basis of C/\mathfrak{m} or

$$C/\mathfrak{m} = \bigoplus_{i=1}^t K\gamma_i, \quad L = \bigoplus_{i=1}^t Kc_i, \quad c_i := \sigma(\gamma_i). \quad (20)$$

For the algorithm we need several effective constructions for finite C -modules which are available for the relevant cases of the introduction by means of Gröbner basis algorithms. The *socle* of the module N is

$$\mathrm{So}(N) := (0 : \mathfrak{m})_N := \{x \in N \mid \mathfrak{m}x = 0\}, \quad Cx = Lx \quad \text{for } x \in \mathrm{So}(N). \quad (21)$$

If the module N is not zero nor is its socle.

ALGORITHM 12. We construct an isomorphic K -linear differential operator $\Phi: N \cong (C/\mathfrak{m})^s$ by means of an L -basis x_1, \dots, x_s of N such that all

$$N_k := \bigoplus_{i=1}^k Lx_i, \quad k = 1, \dots, s,$$

are C -submodules of N . Assume that x_1, \dots, x_k , $k < s$, have already been constructed inductively. Then

$$N_k := \bigoplus_{i=1}^k Lx_i = \sum_{i=1}^k Cx_i \quad \text{and} \quad N/N_k \neq 0;$$

hence

$$\text{So}(N/N_k) = (0 : \mathfrak{m})_{N/N_k} = (N_k : \mathfrak{m})_{N/N_k} \neq 0.$$

Choose any $x_{k+1} \in (N_k : \mathfrak{m})_N \setminus N_k$. Then x_1, \dots, x_{k+1} are L -linearly independent and

$$N_{k+1} = N_k \oplus Lx_{k+1} = N_k + Cx_{k+1} \quad \text{since } \mathfrak{m}x_{k+1} \subseteq N_k.$$

We thus obtain the decomposition $N = N_s = \bigoplus_{i=1}^s Lx_i$ and the L -isomorphism

$$\Phi: N \cong L^s \cong (C/\mathfrak{m})^s,$$

$$x = \sum_{i=1}^s \lambda_i x_i \mapsto (\lambda_1, \dots, \lambda_s)^\top \mapsto (\overline{\lambda_1}, \dots, \overline{\lambda_s})^\top.$$

With (20) we obtain the K -linear differential operator of order m

$$\Phi: N = \bigoplus_{i=1}^s \bigoplus_{j=1}^t Kc_j x_i \cong (C/\mathfrak{m})^s,$$

$$c_j x_i \mapsto \gamma_j \delta_i, \quad \sum_{i,j} \kappa_{ij} c_j x_i \mapsto \left(\sum_{j=1}^t \kappa_{ij} \gamma_j \right)_{i=1, \dots, s}$$

where $\delta_i \in (C/\mathfrak{m})^s$ is the i th standard basis vector.

The L -isomorphism Φ of the preceding algorithm can be evaluated at every $x \in N$ if the basis representation of x can be constructed.

ALGORITHM 13. This algorithm computes the basis representation

$$x = \sum_{i=1}^s \sum_{j=1}^t \kappa_{ij} c_j x_i, \quad \kappa_{ij} \in K, \quad x \in N,$$

by recursion on $i = s, s-1, \dots, 1$. Assume that the κ_{ij} have been constructed for $i = k+1, \dots, s$ such that

$$y := x - \sum_{i=k+1}^s \sum_{j=1}^t \kappa_{ij} c_j x_i \in N_k = N_{k-1} \oplus Lx_k.$$

Then

$$\bar{y} \in N_k/N_{k-1} = C\bar{x}_k, \quad \text{hence } y \equiv cx_k(N_{k-1}) \text{ for some } c \in C.$$

The residue class \bar{c} of c has the K -basis representation

$$\bar{c} = \sum_{j=1}^t \kappa_{kj} \gamma_j \in C/\mathfrak{m} \cong L, \quad \text{hence } \sigma(\bar{c}) = \sum_{j=1}^t \kappa_{kj} c_j,$$

$$\begin{aligned} (c - \sigma(\bar{c}))x_k &\in \mathfrak{m}N_k \subset N_{k-1} \quad \text{and} \quad x - \sum_{i=k+1}^s \sum_{j=1}^t \kappa_{ij} c_j x_i \\ &= y - \sigma(\bar{c})x_k \equiv (c - \sigma(\bar{c}))x_k \equiv 0(N_{k-1}). \end{aligned}$$

Hence the basis representation can be constructed by recursion on i .

Theorem 10 can be formulated as a duality theorem. Indeed, let $E := \text{End}_L(C/\mathfrak{m})$ denote the L -endomorphism (matrix) ring of the L -space C/\mathfrak{m} . The functor

$$M \mapsto D(M) := \text{Hom}_L(M, C/\mathfrak{m})$$

induces the categorical duality

$$\{\text{Finite-dimensional } L\text{-spaces}\}^{\text{op}} \cong \{\text{Finite left } E\text{-modules}\}$$

$$M \mapsto D(M) := \text{Hom}_L(M, C/\mathfrak{m}), \quad \text{Hom}_E(N, C/\mathfrak{m}) \leftarrow N. \quad (22)$$

Here $\text{Hom}_L(M, C/\mathfrak{m})$ is a left E -module via

$$(ef)(x) := e[f(x)] \quad \text{for } e \in E, \quad f \in \text{Hom}_L(M, C/\mathfrak{m}).$$

The canonical Gelfand map

$$\rho: M \rightarrow \text{Hom}_E(\text{Hom}_L(M, C/\mathfrak{m}), C/\mathfrak{m}), \quad \rho(x)(f) := f(x),$$

is an L -isomorphism. If M is a C -module and hence a C -, L -bimodule its dual $\text{Hom}_L(M, C/\mathfrak{m})$ is a C -, E -bimodule with the C -structure $(cf)(x) := f(cx)$. The Gelfand map is even a C -isomorphism.

COROLLARY 14. *The duality $D(-)$ from (22) induces the categorical duality*

$$\{\text{Finite } C\text{-modules}\}^{\text{op}} \cong \{\text{Finite left } C\text{-}E\text{-bimodules}\}$$

$$M \mapsto D(M) := \text{Hom}_L(M, C/\mathfrak{m}) = \text{Diff}_{C/K}(M, C/\mathfrak{m}) \quad (23)$$

with the quasi-inverse $N \mapsto \text{Hom}_E(N, C/\mathfrak{m})$. If the residue field extension $K \subset C/\mathfrak{m}$ is separable the equality

$$D(M) = \text{Hom}_L(M, C/\mathfrak{m}) = \text{Diff}_{C/K}^m(M, C/\mathfrak{m})$$

holds. If the maximal ideal \mathfrak{m} of C is rational or $K = C/\mathfrak{m}$ and $L = K$ then $D(M) = \text{Hom}_K(M, K)$ is the standard dual of the finite K -space M . This case was treated in [8] for cyclic coprimary modules.

4. THE PROOF OF THE MAIN THEOREM

We return to the data of the Introduction and give some more details on its preparatory remarks. We have used the normalization theorem in the explicit form of [13, Th. 14.2]: There are elements

$$\zeta_1, \dots, \zeta_n \in A = F[t], \quad \zeta_j = t_j + f_j(t_{II}) \quad \text{for } j = 1, \dots, d,$$

$$t_{II} := (t_{d+1}, \dots, t_n)$$

such that $F[t]$ is a finite $F[\zeta] = F[\zeta_1, \dots, \zeta_n]$ -module and

$$F[\zeta] \cap J = \sum_{j=d+1}^n F[\zeta] \zeta_j.$$

The polynomials f_j have coefficients in the prime field. If F is infinite they can be chosen linear with coefficients in F . We infer that ζ_1, \dots, ζ_n are algebraically independent over F and that $\zeta_1, \dots, \zeta_d, t_{d+1}, \dots, t_n$ are generators of A , i.e.,

$$A = F[\zeta_I, t_{II}] = F[\zeta_1, \dots, \zeta_d, t_{d+1}, \dots, t_n] = F[\zeta_I][t_{II}] = B[t_{II}],$$

$$B := F[\zeta_I],$$

and

$$B = F[\zeta_I] \cong F[\zeta] / \langle \zeta_{II} \rangle = F[\zeta] / (J \cap F[\zeta]) \rightarrow A/J$$

is a finite homomorphism. The finite A -module M from Theorem 1 is J -coprimary; hence (3) holds according to [2, Ch. IV, Section 2, Prop. 1]. In particular, a power of J annihilates M and thus its minimal exponent $m+1$ with $J^{m+1}M = 0$ or $J^{m+1} \subseteq I$ exists. Since A/J is a finite B -module so are all factors J^{i-1}/J^i , A/J^i and A/I and M too. The monoid $S = B \setminus \{0\} \subseteq A \setminus J$ consists of non-zero-divisors of A/J , and hence the finite monomorphism $B \rightarrow A/J$ induces the finite monomorphism

$$K := S^{-1}B = F(\zeta_I) \rightarrow S^{-1}(A/J)$$

of integral domains. Since K is a field so is $S^{-1}(A/J)$, and this signifies that the latter is indeed the quotient field of A/J as already stated in (2):

$$S^{-1}(A/J) = S^{-1}A/S^{-1}J = A_J/J_J = \text{quot}(A/J) = k(J).$$

In particular, $S^{-1}J$ is a *maximal* ideal of $S^{-1}A = F(\zeta_I)[t_{II}]$. Since A/I is a finite B -module the algebra $C := S^{-1}(A/I)$ is finite dimensional over K , and the equations (5) and (6) hold. Likewise, $S^{-1}M$ is a finite-dimensional K -vector space which contains M since $S(\subseteq A \setminus J)$ consists of non-zero-divisors of M . In particular, it is $S^{-1}J$ -coprimary with the minimal exponent $m + 1$ such that $(S^{-1}J^{m+1})(S^{-1}M) = 0$. For any finite C -module N the localization $N_{\mathfrak{m}}$ coincides with N since $C \setminus \mathfrak{m} = U(C)$ consists of the units of C . This applies to C , C/\mathfrak{m} , and $S^{-1}M$ and furnishes

$$\begin{aligned} C &= S^{-1}A/S^{-1}I = F(\zeta_I)[t_{II}]/F(\zeta_I)I = C_{\mathfrak{m}} \\ &= (S^{-1}A/S^{-1}I)_{S^{-1}J/S^{-1}I} = A_J/I_J, \\ C/\mathfrak{m} &= (C/\mathfrak{m})_{\mathfrak{m}} = A_J/J_J = k(J), \\ S^{-1}M &= (S^{-1}M)_{\mathfrak{m}} = (S^{-1}M)_{S^{-1}J/S^{-1}I} = M_J. \end{aligned}$$

The considerations of Section 3 are applicable to the finite C -module $S^{-1}M$ over the finite-dimensional local K -algebra C .

Proof of the main theorem 1. (i) The data are those from the introduction with the specifications from above. In particular, we use the separable field extension

$$K \subset L := C_{\text{sep}} = (F(\zeta_I)[t_{II}]/F(\zeta_I)I)_{\text{sep}} \cong (C/\mathfrak{m})_{\text{sep}} = k(J)_{\text{sep}}$$

and the length or multiplicity of $S^{-1}M$ as $S^{-1}A$ -, A_J -, or C -module:

$$s := \text{length}_C(S^{-1}M) = \text{length}_{A_J}(M_J) = [S^{-1}M : L]/[k(J) : L].$$

We choose any L -isomorphism, for instance, by means of Algorithm 12,

$$\Phi: S^{-1}M \cong k(J)^s = S^{-1}(A/J)^s.$$

Due to Theorem 10 this is a K -linear differential operator, say, of order p which, in general, is much greater than the exponent m . Hence

$$\begin{aligned} \Phi &\in \text{Diff}_{C/K}^p(S^{-1}M, S^{-1}(A/J)^s) = \text{Diff}_{S^{-1}A/S^{-1}B}^p(S^{-1}M, S^{-1}(A/J)^s) \\ &= \text{Diff}_{A/B}^p(S^{-1}M, S^{-1}(A/J)^s). \end{aligned}$$

By (11) the composition

$$\bar{D} = (\bar{D}_1, \dots, \bar{D}_q): A^q \xrightarrow{\text{can}} M = A^q/U \subset S^{-1}M \xrightarrow{\Phi} S^{-1}(A/J)^s$$

and its components

$$\begin{aligned}\bar{D}_k: A &\rightarrow S^{-1}(A/J)^s, & \bar{D}_k(P) &= \Phi(\overline{P\delta_k}), \\ \overline{P\delta_k} &:= (0, \dots, 0, P, 0, \dots, 0) + U \in M,\end{aligned}$$

are also B -linear differential operators of order p . The algebra $A = B[t_{II}] = B[t_{d+1}, \dots, t_n]$ is polynomial so that by (16) \bar{D} is uniquely determined by the images

$$\begin{aligned}\bar{D}_k(t_{II}^\alpha) &= \Phi(\overline{t_{II}^\alpha \delta_k}) \in S^{-1}(A/J)^s, & t_{II}^\alpha &:= t_{d+1}^{\alpha_{d+1}} * \dots * t_n^{\alpha_n}, \\ \alpha &= (\alpha_{d+1}, \dots, \alpha_n) \in \mathbb{N}^{n-d}, & |\alpha| &:= \alpha_{d+1} + \dots + \alpha_n \leq p, \\ & & k &= 1, \dots, q.\end{aligned}\tag{24}$$

The finitely many elements from (24) have a common denominator $s_0 \in B$. Choose vectors $y_k^\alpha \in A^s$ such that

$$\begin{aligned}\overline{y_k^\alpha} &= s_0 \Phi(\overline{t_{II}^\alpha \delta_k}) \in (A/J)^s \quad \text{for all } \alpha \in \mathbb{N}^{n-d}, \quad |\alpha| \leq p, \\ & k = 1, \dots, q.\end{aligned}\tag{25}$$

Again due to (16) there are unique B -linear differential operators $D_k: A \rightarrow A^s$ such that

$$D_k(t_{II}^\alpha) = y_k^\alpha \in A^s \quad \text{for all } \alpha \in \mathbb{N}^{n-d}, \quad |\alpha| \leq p, \quad k = 1, \dots, q,\tag{26}$$

and then the differential operator

$$D := (D_1, \dots, D_s): A^q \rightarrow A^s, \quad D(v_1, \dots, v_q) := \sum_{k=1}^q D_k(v_k),$$

has the properties asserted in Theorem 1.

(ii) If the residue field extension $K \subset k(J)$ is separable the differential operator Φ is of order $p = m$ according to Theorem 10 (where $J^{m+1}M = 0$) and the same holds for the constructed D by definition.

(iii) An arbitrary B -linear noetherian differential operator $D: A^q \rightarrow A^s$, $s := \text{length}_{A_J}(M_J)$, for M or U induces a B -monomorphism $D_{\text{ind}, 1}$ and a K -isomorphism $D_{\text{ind}, 2}$ such that the diagram

$$\begin{array}{ccccc} A^q & \xrightarrow{\text{can}} & M = A^q/U & \xrightarrow{\text{inj}} & S^{-1}M \\ \downarrow D & & \downarrow D_{\text{ind}, 1} & & \downarrow D_{\text{ind}, 2} \\ A^s & \xrightarrow{\text{can}} & (A/J)^s & \xrightarrow{\text{inj}} & k(J)^s \end{array}$$

commutes. Indeed this follows from

$$U = \{v \in A^q; \text{can} \circ D(v) = 0\} \quad \text{and} \quad [S^{-1}M : K] = [S^{-1}(A/J)^s : K].$$

Moreover $D_{\text{ind}, 2}$ is a differential operator since D is one, and this implies by Theorem 10 that $D_{\text{ind}, 2}$ is indeed L -linear. Another noetherian differential operator \tilde{D} for M likewise induces the L -isomorphism $\tilde{D}_{\text{ind}, 2}$. The L -automorphism $\Psi := \tilde{D}_{\text{ind}, 2} \circ D_{\text{ind}, 2}^{-1}$ is the unique L -linear map or K -linear differential operator satisfying

$$\tilde{D}_{\text{ind}, 2} = \Psi \circ D_{\text{ind}, 2} \quad \text{or} \quad \text{can} \circ \tilde{D} = \Psi \circ \text{can} \circ D.$$

■

ALGORITHM 15. The preceding theorem contains the following algorithm for the computation of the noetherian operator for M if the residue field extension $K \subset k(J)$ is separable and $m + 1$ is the nilpotency exponent with $J^{m+1}M = 0$

(i) Construct the L -isomorphism $\Phi: S^{-1}M \cong S^{-1}(A/J)^s$ by means of Algorithm 12.

(ii) Compute the images

$$\Phi(\overline{t_H^\alpha \delta_k}) \in S^{-1}(A/J)^s \quad \text{for all } \alpha \in \mathbb{N}^{n-d}, \quad |\alpha| \leq m, \quad k = 1, \dots, q,$$

with Algorithm 13 and choose a common denominator s_0 of these images and representatives $y_k^\alpha \in A^s$ such that (25) is satisfied.

(iii) Then the differential operators D_k from (26) give rise to the noetherian differential operator

$$D = (D_1, \dots, D_s): A^q \rightarrow A^s, \quad (v_1, \dots, v_q) \mapsto \sum_{k=1}^q D_k(v_k),$$

for U where $D_k: A \rightarrow A^s$ has the explicit form

$$D_k(P) = \sum_{k=1}^q \sum_{\beta \leq \alpha, |\alpha| \leq m} (D^\alpha P) \binom{\alpha}{\beta} (-t)^{\alpha-\beta} y_k^\beta$$

and where $D^\alpha = (1/\alpha!)(\partial^{|\alpha|}/\partial t_H^\alpha)$ in characteristic zero.

EXAMPLE 16. Let

$$F := \mathbb{Q}, \quad A = \mathbb{Q}[t_1, t_2], \quad J = \langle t_2^2 + t_1^3 \rangle, \quad I = J^2 = \langle (t_2^2 + t_1^3)^2 \rangle,$$

$$M = A/I = \mathbb{Q}[t_1, t_2]/\langle (t_2^2 + t_1^3)^2 \rangle, \quad B = \mathbb{Q}[t_1] \subset A = B[t_2], \quad t_H = t_2,$$

$$K = \mathbb{Q}(t_1) \subset k(J) = \mathbb{Q}(t_1)[t_2]/\langle t_2^2 + t_1^3 \rangle = K \oplus K\tau,$$

$$\tau := \overline{t_2} =: \gamma_2, \quad \gamma_1 := 1,$$

$$C = S^{-1}M = \mathbb{Q}(t_1)[t_2]/\langle (t_2^2 + t_1^3)^2 \rangle \supset \mathfrak{m} = \langle \overline{t_2} + t_1^3 \rangle / \langle (t_2^2 + t_1^3)^2 \rangle.$$

It is easily seen that for these data the operator

$$\left(\begin{array}{c} 1 \\ \partial/\partial t_2 \end{array} \right): \quad \mathbb{Q}[t] \rightarrow \mathbb{Q}[t]^2$$

is a noetherian operator for I [16, Ch. IV, Section 4, Prop. 3]. We use Algorithm 15 to construct another operator. The next computations take place in $C = \mathbb{Q}(t_1)[t_2]/\langle (t_2^2 + t_1^3)^2 \rangle$. We write t_1 and t_2 for the residue classes in C too to avoid a cumbersome notation.

(i) First we construct the section $\sigma: k(J) \cong C_{\text{sep}} =: L$ of the canonical map and then conclude

$$L = K \oplus K\sigma(\tau) = Kc_1 \oplus Kc_2, \quad c_1 = \sigma(\gamma_1) = 1,$$

$$c_2 = \sigma(\gamma_2) = \sigma(\tau).$$

The element $\sigma(\tau)$ is computed with the algorithm contained in the proof of Lemma 7. The minimal polynomial of $\tau = \bar{t}_2$ over $\mathbb{Q}(t_1)$ is of course $f = X^2 + t_1^3$; hence $f' = 2X$ and

$$c_2 = t_2 - f'(t_2)^{-1} f(t_2) = t_2 - (2t_2)^{-1}(t_2^2 + t_1^3) \in C.$$

The defining equation $(t_2^2 + t_1^3)^2 = 0 \in C$ implies

$$t_2^{-1} = -t_1^{-6}t_2(t_2^2 + 2t_1^3) \quad \text{and} \quad c_2 = \sigma(\tau) = \frac{1}{2}t_1^{-3}t_2(t_2^2 + 3t_1^3).$$

(ii) The construction of the L -basis x_1 and x_2 of C is trivial; indeed

$$x_1 := t_2^2 + t_1^3 \in \mathfrak{m} \subset C, \quad x_2 := 1.$$

There in results the L -isomorphism

$$\Phi: C \cong k(J)^2, \quad \Phi(c_j x_i) = \gamma_j \delta_i,$$

$$\Phi(1) = \Phi(c_1 x_2) = \gamma_1 \delta_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

$$\Phi(t_2^2 + t_1^3) = \Phi(c_1 x_1) = \gamma_1 \delta_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

$$\Phi(\sigma(\tau)) = \Phi(c_2 x_2) = \gamma_2 \delta_2 = \begin{pmatrix} 0 \\ \tau \end{pmatrix},$$

$$\Phi(\sigma(\tau)(t_2^2 + t_1^3)) = \Phi(c_2 x_1) = \gamma_2 \delta_1 = \begin{pmatrix} \tau \\ 0 \end{pmatrix}.$$

The element $t_2 \in C$ is decomposed as

$$t_2 = \sigma(\tau) + t_2 - \sigma(\tau) \in C = L \oplus \mathfrak{m}, \quad \tau = \bar{t}_2.$$

But

$$\begin{aligned}
 t_2 - \sigma(\tau) &= t_2 - \frac{1}{2}t_1^{-3}t_2(t_2^2 + 3t_1^3) = \frac{1}{2}t_1^{-3}(2t_1^3t_2 - t_2^3 - 3t_1^3t_2) \\
 &= -\frac{1}{2}t_1^{-3}t_2(t_2^2 + t_1^3) = -\frac{1}{2}t_1^{-3}t_2x_1 = -\frac{1}{2}t_1^{-3}\sigma(\tau)x_1 \\
 &= -\frac{1}{2}t_1^{-3}c_2x_1;
 \end{aligned}$$

hence

$$\begin{aligned}
 \Phi(t_2) &= \Phi(\sigma(\tau)) + \Phi(t_2 - \sigma(\tau)) = \Phi(c_2x_2) - \frac{1}{2}t_1^{-3}\Phi(c_2x_1) \\
 &= \begin{pmatrix} 0 \\ \tau \end{pmatrix} - \frac{1}{2}t_1^{-3}\begin{pmatrix} \tau \\ 0 \end{pmatrix} = \begin{pmatrix} -t_1^{-3}\tau/2 \\ \tau \end{pmatrix}.
 \end{aligned}$$

(iii) A common denominator of $\Phi(1)$ and $\Phi(t_2)$ is t_1^3 . Therefore the $\mathbb{Q}[t_1]$ -linear differential operator $D: \mathbb{Q}[t] \rightarrow \mathbb{Q}[t]^2$ of order one with

$$D(1) = \begin{pmatrix} 0 \\ t_1^3 \end{pmatrix}, \quad D(t_2) = \begin{pmatrix} -t_2/2 \\ t_1^3t_2 \end{pmatrix},$$

determines I . It is given by

$$\begin{aligned}
 D(P) &= \sum_{\beta \leq \alpha \leq 1} (D^\alpha P) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} (-t_2)^{\alpha-\beta} D(t^\beta) \\
 &= PD(1) + \partial P / \partial t_2 [(-t_2)D(1) + D(t_2)] \\
 &= (P - t_2 \partial P / \partial t_2) \begin{pmatrix} 0 \\ t_1^3 \end{pmatrix} + \partial P / \partial t_2 \begin{pmatrix} -t_2/2 \\ t_1^3t_2 \end{pmatrix} \\
 &= \begin{pmatrix} -(t_2/2) \partial P / \partial t_2 \\ t_1^3 P \end{pmatrix} = \begin{pmatrix} 0 & -t_2/2 \\ t_1^3 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ \partial / \partial t_2 \end{pmatrix} (P).
 \end{aligned}$$

But the matrix

$$\begin{pmatrix} 0 & -t_2/2 \\ t_1^3 & 0 \end{pmatrix}$$

is invertible modulo J since its determinant $t_1^3t_2/2 \pmod{J} = -\tau^3/2$ is invertible in $k(J) = K \oplus K\tau$. Hence

$$P \in I \Leftrightarrow D(P) \equiv 0 \pmod{J} \Leftrightarrow \begin{pmatrix} 1 \\ \partial / \partial t_2 \end{pmatrix} (P) \equiv 0 \pmod{J}.$$

The connection of Theorem 1 with M. Noether's *Fundamentalsatz* is the following. The algebra $C = S^{-1}(A/I)$ in the proof of the theorem can be replaced by the local algebra

$$C_J := S^{-1}(A/J^{m+1}) = A_J/J_J^{m+1}$$

with the maximal ideal $\mathfrak{m}_J = J_J/J_J^{m+1}$ and the separable part $L_J := (C_J)_{\text{sep}} \cong (A_J/J_J)_{\text{sep}}$. Since $J^{m+1}A^q \subseteq U$ we obtain

$$S^{-1}M = M_J = (A^q/U)_J = (A^q/J^{m+1}A^q)_J/(U/J^{m+1}A^q)_J = C_J^q/C_JU$$

and the monomorphism

$$M = A^q/U \rightarrow S^{-1}M = C_J^q/C_JU, \quad v + U \mapsto \bar{v} + C_JU,$$

$$v = (v_1, \dots, v_q) \in A^q, \quad \bar{v} := (\bar{v}_1, \dots, \bar{v}_q) \in (A_J/J_J^{m+1})^q.$$

In particular, the equivalence

$$v \equiv 0 \pmod{U} \Leftrightarrow \bar{v} \equiv 0 \pmod{C_JU} \quad (27)$$

holds. V. d. Waerden [19, p. 69, p. 78] calls this equivalence M. Noether's *Fundamentalsatz* or rather its generalization to arbitrary, not necessarily primary submodules U of A^q (see (28) below). Its significance lies in the fact that it reduces the membership problem $\{v \in U\}$ to the simple K -linear algebra problem $\{\bar{v} \in C_JU\}$ since C_J^q is a *finite-dimensional* vector-space over K . Remark that today the membership problem can be solved by means of Buchberger's Gröbner basis algorithm. Obviously Eq. (27) can be expressed as

$$v \equiv 0 \pmod{U} \Leftrightarrow \Phi(\bar{v} + C_JU) = 0$$

where $\Phi: S^{-1}M \cong (A_J/J_J)^s$ is an arbitrary L_J -isomorphism. The simple, but decisive additional observation of Theorem 1 is that Φ is always a K -linear differential operator which can be lifted to a B -linear differential operator $D: A^q \rightarrow A^s$.

If U is an arbitrary submodule of A^q one first computes a primary decomposition

$$U = \bigcap_{J \in \text{Ass}(M)} U(J), \quad \text{Ass}(A^q/U(J)) = \{J\}$$

and then for each primary component $U(J)$ a $B(J)$ -linear differential operator

$$D_J: A^q \rightarrow A^{s(J)}, \quad s(J) := \text{length}_{A_J}(A_J^q/U(J)_J), \quad \text{such that}$$

$$U(J) = \{v \in A^q; D_J(v) | \text{Var}(J) = 0\}$$

where the polynomial algebra $B(J) \subset A = F[t]$ according to Theorem 1 depends on J . Then

$$\begin{aligned} v \equiv 0 \pmod{U} &\Leftrightarrow \text{For all } J \in \text{Ass}(M): \bar{v} \equiv 0 \pmod{C_J U} \\ &\Leftrightarrow \text{For all } J \in \text{Ass}(M): D_J(v) | \text{Var}(J) = 0. \end{aligned} \quad (28)$$

The first equivalence is the most general form of Noether's *Fundamentalsatz* [19, p. 78], whereas the second contains the general existence of noetherian operators [16, pp. 174, 178].

Remark 17. We discuss some further constructivity aspects of Algorithms 12, 13, and 15 and refer to Vasconcelos' book [18] for the needed effective computations. Noether normalization and primary decomposition are discussed in [loc.cit, Section 2.3 resp. Ch. 3]. Gröbner basis computations over $S^{-1}A = K[t_{II}] = F(\zeta_I)[t_{II}]$ can be reduced to those over $A = F[\zeta_I, t_{II}]$ [loc. cit., p. 20]. Computations for the finite field extension

$$K = F(\zeta_I) \subset k(J) = F(\zeta_I)[\overline{t_{d+1}}, \dots, \overline{t_n}]$$

are reduced to calculations in the polynomial algebra $F(\zeta_I)[X]$ in one indeterminate X . The construction of the section $\sigma: k(J) \cong C_{\text{sep}}$ according to Lemma 7 requires the inversion of elements in the unit group $U(C)$. But if $f \in K[t_{II}]$ is not contained in the maximal ideal $S^{-1}J = KJ$ the Gröbner basis algorithm yields

$$\begin{aligned} 1 = gf + h \in K[t_{II}] &= K[t_{II}]f + KJ^{m+1} \quad \text{and} \\ \bar{g} = (\bar{f})^{-1} &\in C = K[t_{II}]/KI. \end{aligned}$$

Computations in and over the local Artin algebra

$$C = S^{-1}(A/I) = F(\zeta_I)[t_{II}]/F(\zeta_I)I$$

are the subject of [loc.cit, Ch. 4], and make the calculations of the algorithms of this paper effective.

REFERENCES

1. J. E. Björk, "Rings of Differential Operators," North-Holland, Amsterdam, 1979.
2. N. Bourbaki, "Commutative Algebra," Hermann, Paris, 1972.
3. R. Brommer, High order derivations and primary ideals to regular prime ideals, *Arch. Math.* **46** (1986), 511–521.
4. M. Demazure and P. Gabriel, "Groupes Algébrique," Masson, Paris, 1970.
5. L. Ehrenpreis, "Fourier Analysis in Several Complex Variables," Wiley-Interscience, New York, 1970.

6. W. Gröbner, Über eine neue idealtheoretische Grundlegung der algebraischen Geometrie, *Math. Ann.* **115** (1938), 333–358.
7. W. Gröbner, “La théorie des idéaux et la Géométrie algébrique,” Colloque de Géométrie Algébrique, Liège, 1952.
8. W. Gröbner, “Algebraische Geometrie II,” Bibliographisches Institut, Mannheim, 1970.
9. P. Hackmann, $E(A/P)$, preprint Lith-Mat-R-96-05, Department of Mathematics, Linköping University, S-58183 Sweden.
10. L. Hörmander, “An Introduction to Complex Analysis in Several Variables,” North-Holland, Amsterdam, 1973.
11. M. G. Marinari, H. M. Möller, and T. Mora, On multiplicities in polynomial system solving, *Trans. Amer. Math. Soc.* **348** (1996), 3283–3221.
12. H. Matsumura, “Commutative Ring Theory,” Cambridge Univ. Press, Cambridge, UK, 1986.
13. M. Nagata, “Local Rings,” Interscience, New York, 1962.
14. U. Oberst, Multidimensional constant linear systems, *Acta Appl. Math.* **20** (1990), 1–175.
15. U. Oberst, Variations on the fundamental principle for linear systems of partial differential and difference equations with constant coefficients, *Appl. Algebra Engrg. Comm. Comput.* **6** (1995), 211–243.
16. V. P. Palamodov, “Linear Differential Operators with Constant Coefficients,” Springer-Verlag, Berlin, 1970.
17. J. P. Serre, “Corps Locaux,” Hermann, Paris, 1962.
18. W. V. Vasconcelos, “Computational Methods in Commutative Algebra and Algebraic Geometry,” Springer-Verlag, Berlin, 1998.
19. B. L. Van der Waerden, “Moderne Algebra, Zweiter Teil,” Springer-Verlag, Berlin, 1931.
20. J. Wood, U. Oberst, E. Roger, and D. Owens, A behavioural approach to the pole structure of 1D and nD systems, *SIAM J. Contr. Opt.*, to appear.